National Aeronautics and
Space Administration

NOT MEASUREMENT
SENSITIVE

NASA-STD-2820
July 29, 2001

ENCRYPTION AND DIGITAL SIGNATURE STANDARDS

NASA TECHNICAL STANDARD

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY) 29-07-2001	2. REPORT TYPE	3. DATES COVERED (FROM - TO) xx-xx-2001 to xx-xx-2001

4. TITLE AND SUBTITLE
Encryption and Digital Signature Standards NASA-STD-2820
Unclassified

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Holcomb, Lee B. ;

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME AND ADDRESS
Booz Allen & Hamilton
8283 Greensboro Drive
McLean, VA22102

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS
NASA
,

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Encryption can be used to safeguard transmitted data, minimize unauthorized access to data during storage, and authenticate the identities of users, terminals and computers. Data encryption shall be used whenever it is the most appropriate method available to protect the confidentiality or integrity of data. Estimating the costs, determining the acceptable level of risk, and deciding to employ cryptographic protections are management functions of the authority responsible for the data. A guide for when and what encryption should be used is contained in the document entitled: Guidance on the Use of Encryption and Digital Signatures for the Protection of Sensitive but Unclassified Information (currently available only within NASA).

15. SUBJECT TERMS
IATAC Collection; encryption; digital signature standards

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Public Release	18. NUMBER OF PAGES 15	19. NAME OF RESPONSIBLE PERSON Fenster, Lynn lfenster@dtic.mil
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 703767-9007 DSN 427-9007

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 074-0188*

1. AGENCY USE ONLY (Leave blank)	**2. REPORT DATE** 7/29/2001	**3. REPORT TYPE AND DATES COVERED** Report 7/29/2001

4. TITLE AND SUBTITLE
Encryption and Digital Signature Standards NASA-STD-2820

5. FUNDING NUMBERS

6. AUTHOR(S)
Lee B. Holcomb

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Booz Allen & Hamilton
8283 Greensboro Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

National Aeronautics and Space Administration

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT *(Maximum 200 Words)*

Encryption can be used to safeguard transmitted data, minimize unauthorized access to data during storage, and authenticate the identities of users, terminals and computers. Data encryption shall be used whenever it is the most appropriate method available to protect the confidentiality or integrity of data. Estimating the costs, determining the acceptable level of risk, and deciding to employ cryptographic protections are management functions of the authority
responsible for the data. A guide for when and what encryption should be used is contained in the document entitled: Guidance on the Use of Encryption and Digital Signatures for the Protection of Sensitive but Unclassified Information (currently available only within NASA).

14. SUBJECT TERMS
IATAC Collection, encryption, digital signature standards,

15. NUMBER OF PAGES
14

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	**18. SECURITY CLASSIFICATION OF THIS PAGE** UNCLASSIFIED	**19. SECURITY CLASSIFICATION OF ABSTRACT** UNCLASSIFIED	**20. LIMITATION OF ABSTRACT** UNLIMITED

FOREWORD

This standard is approved for use by NASA Headquarters and all NASA Centers and is intended to provide a common framework for consistent practices across NASA programs.

The material covered in this standard is based on the consensus judgment of the NASA Chief Information Officer's (CIO) Board. The purpose of this standard is to establish the minimum encryption and digital signature standards required to support interoperability, establish interface and product standards for components of NASA's IT Security and e-commerce posture, and establish reporting metrics for determining overall NASA interoperability.

Requests for information, corrections, or additions to this standard should be directed to the Ames Research Center (ARC), the Principal Center for Information Technology Security, Code JT, MS 233-17, Moffett Field, CA 94035. Requests for additional copies of this standard should be sent to NASA Technical Standards Program Office, ED41, MSFC, AL,35812 (telephone 256-544-2448). This and other NASA standards may be viewed and downloaded, free-of-charge, from our NASA Standards Homepage: http://standards.nasa.gov.

Lee B. Holcomb
Chief Information Officer

This Page Left Blank Intentionally

TABLE OF CONTENTS

PARAGRAPH PAGE

TABLE OF CONTENTS

PARAGRAPH PAGE

TABLES

TABLE PAGE

ENCRYPTION AND DIGITAL SIGNATURE STANDARDS

1. INTRODUCTION

Encryption can be used to safeguard transmitted data, minimize unauthorized access to data during storage, and authenticate the identities of users, terminals and computers. Data encryption shall be used whenever it is the most appropriate method available to protect the confidentiality or integrity of data. Estimating the costs, determining the acceptable level of risk, and deciding to employ cryptographic protections are management functions of the authority responsible for the data. A guide for when and what encryption should be used is contained in the document entitled: *Guidance on the Use of Encryption and Digital Signatures for the Protection of Sensitive but Unclassified Information* (currently available only within NASA).

This document was developed to establish interoperable standards for protecting sensitive or valuable data within NASA computer systems and networks. When there is a need for secure transactions, individuals or other entities interacting with NASA should have reasonable assurance that:

a) the information sender and recipient will both be identified uniquely so the parties know where the information is coming from and where it is going (identification and authentication);
b) the transmitted information was not altered deliberately or inadvertently (data integrity);
c) the sender's identity is inextricably bound to the information (technical non-repudiation); and
d) the information will be protected from unauthorized access (confidentiality or privacy).

NASA has requirements for the recovery of encrypted data. Two critical elements of recovery are paramount: (a) the technical and procedural capability to recover encrypted data; and (b) the recovery of encrypted data must not result in any copies or changes being made of the private keys used for digital signatures.

In addition, NASA is required to comply with the Government Paperwork Elimination Act and other relevant laws and regulations. These requirements can be met through the use of digital signatures.

An electronic document or file may be digitally signed using a party's private signature key, creating a "digital signature" that is stored and linked with the document. At a later date, anyone can validate the signature on the document using the public key from the digital certificate issued to the signer. Validating the digital signature not only confirms who signed it, but also ensures that there have been no alterations to the document since it was signed. Similarly, an e-mail message may be digitally signed using commonly available client software that implements an open standard for this purpose, such as Secure Multipurpose Internet Mail Extensions (S/MIME). Validating the signature on the e-mail can help the recipient know with confidence who sent it, and that it was not altered during transmission.

An electronic signature must:

a) Be unique to the signer
b) Be under the signer's sole control
c) Be capable of verification
d) Be linked to the data covered by the signature in such a manner that if the data are changed, the signature will not be validated, and
e) Conform to NIST's use of algorithms, techniques, and other requirements approved by NIST.

Relevant Federal Guidance:

a) Electronic Signatures in Global and National Commerce Act ("E-SIGN") (Public Law 106-229) – validity of electronic records and signatures for commerce
b) Government Paperwork Elimination Act (GPEA) (Public Law 105-277) – requires Federal Agencies, by October 21, 2003, to allow individuals or entities that deal with an Agency the option to submit information or perform transactions with an Agency electronically, when practicable, and to maintain records electronically, when practicable
c) NARA, Records Management Guidance for Agencies Implementing Electronic Signature Technologies, dated October 18, 2000
d) Privacy Act of 1974
e) Computer Matching and Privacy Protection Act of 1988

2. SCOPE

2.1. Purpose and Scope. This standard establishes required technologies and practices for encryption and digital signatures within the agency and establishes interface and product standards for securing NASA's Information Technology (IT) data and information. This standard also establishes reporting metrics for determining overall NASA compliance with Federal and NASA IT security standards.

2.2. Applicability. All Center CIO's are required to ensure that all NASA employees are securing systems, data, and information in a manner that is commensurate with the risk associated with those systems, data, and information. Each Center will determine how best to integrate these technologies and practices for encryption and digital signatures within their infrastructures.

3. ACRONYMS AND DEFINITIONS

3.1. Acronyms

ADK	Additional Key Decryption
AES	Advanced Encryption Standard
CA	Certificate Authority
CIO	Chief Information Officer
COTS	Commercial "Off-the-Shelf" product
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
FIPS	Federal Information Processing Standard

FTP	File Transfer Protocol
GSS-API	Generic Security Service Application Program Interface
IETF	Internet Engineering Task Force
IPsec	Internet Protocol Security
IT	Information Technology
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
PCITS	Principle Center for Information Technology Security
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
RA	Registration Authority
SHA-1	Secure Hash Algorithm
S-MIME	Secure Multipurpose Internet Mail Extension
SSH	Secure Shell
SSL	Secure Socket Layer
VPN	Virtual Private Network

3.2. Definitions

3.2.1. AES. The Advanced Encryption Standard (AES) will be a new Federal Information Processing Standard (FIPS) Publication that will specify a cryptographic algorithm for use by U.S. Government organizations to protect sensitive (unclassified) information. The National Institute of Standards and Technology (NIST) also anticipates that the AES will be widely used on a voluntary basis by organizations, institutions, and individuals outside of the U.S. Government - and outside of the United States-in some cases. The AES will become official after the 90-day public comment period concludes, after NIST makes appropriate changes to the Draft FIPS, and after the Secretary of Commerce approves the FIPS. NASA will update the Interface Standard from Triple DES to the AES as soon as it is approved as a standard, and commercial products support it. After sufficient time is allowed for incorporation of the AES into commercial products and included into the NIST Approved Products List, NASA will update the NASA Encryption and Digital Signature Standards, NASA-STD-2820.

3.2.2. PGP. Pretty Good Privacy (PGP) is based on the public-key method, which uses two keys. One is a public key that can be disseminated to individuals who wish to send a message. The other is a private key that is used to decrypt messages that are received. The use of PGP requires using ADK (a method of key recovery) when used within NASA and operated in the FIPS mode using the listed FIPS-approved algorithms, such as Triple DES.

3.2.3. PKI. Public Key Infrastructure (PKI) is the framework and service that provides for the generation, production, distribution, control, accounting and destruction of public key certificates. PKI is the term generally used to describe the laws, policies, standards, and software that regulate or manipulate certificates and public and private keys. Public key technology is also called "asymmetric cryptography." In a typical PKI, two key-pairs are generated by or for each user. One key-pair is for digital signatures and authentication, and the other key-pair is for encryption. Each key-pair comprises two keys. These "keys" are very large numbers, up to 150 to 300 digits in length and are subtlety, mathematically linked. In each key-pair, one key is kept private, and the other made public. A trusted party cryptographically binds the public key to the person's identity by digitally signing the certificate. These trusted parties are called Certification Authorities or "CA"s. The digital signature on the certificate ensures that any unauthorized alteration of either the identity or the public key will be detected.

3.2.4. VPN. A Virtual Private Network (VPN) is a network that is constructed by using "virtual" networks layered over physical networks to connect nodes. For example, there are a number of systems that enable one to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network, that the data cannot be intercepted, and that it follows the IPsec protocols.

3.2.5. Smart Card Token. A smart card token is a small electronic device that contains electronic memory and an embedded integrated circuit (IC). It is comprised of a microprocessor (CPU), ROM, RAM, EEPROM and a serial communication interface. The built-in smartness enables a smart card to protect information stored in it from unauthorized access. The device performs Private Key Encryption. The smart card token follows the International Organization for Standardization standard for smart cards (ISO 7816).

3.2.6. Smart Card. A smart card is a small electronic device about the size of a credit card that contains electronic memory, and possibly an embedded IC. Smart cards containing an IC are sometimes called Integrated Circuit Cards (ICCs). A smart card is comprised of a microprocessor (CPU), ROM, RAM, EEPROM and a serial communication interface. The built-in smartness enables a smart card to protect information stored in it from unauthorized access. The device performs Private Key Encryption. The smart card follows the International Organization for Standardization standard for smart cards (ISO 7816).

3.2.7. Digital Certificates. X.509 digital certificates contain the applicant's public key and a variety of other identification information.

3.2.8. Digital Signature. A digital signature is a digital code that can be attached to an electronically transmitted message that uniquely identifies the sender/signer. A digital signature is computed using a set of rules and a set of parameters, such that the identity of the signatory and integrity of the data can be verified. An algorithm provides the capability to generate and verify signatures. Like a written signature, the purpose of a digital signature is to guarantee that the individual sending is really is who he or she claims to be. Digital signatures are especially important for electronic commerce and are a key component of most authentication schemes. To be active, digital signatures must not be forgeable.

3.2.9. SHA-1. Secure Hash Algorithm (SHA-1) can be used to generate a condensed representation of a message called a "message digest." The SHA-1 is required for use with the Digital Signature Algorithm (DSA) as specified in the Digital Signature Standard (DSS) and whenever a secure hash algorithm is required for Federal applications. The SHA-1 is used by the transmitter and the intended receiver of a message in computing and verifying a digital signature. SHA-1 is specified in FIPS 180-1.

3.2.10. IPsec. IPsec is a suite of protocols defined by a set of Request for Comments (RFC) that can be used to create secure communications as defined in Internet standards RFCs 2630, 2631, 2632, 2633, and 2634.

3.2.11. Freeware. Freeware is copyrighted software given away for free by the author. Although it is available for free, the author retains the copyright, which means that users cannot do anything with it that is not expressly allowed by the author. Usually, the author allows people to use the software, but not sell it.

3.2.12. Shareware. These products are available for use typically at a nominal charge with specific license restrictions. Generally, users have the ability to test the product before purchase. Shareware is usually distributed over the Internet from the vendor.

4. DETAILED REQUIREMENTS

4.1. Compliance Requirements. NASA has baselined and approved an initial NASA Integrated IT Architecture, NASA-STD-2814, *Nasa Integrated Information Technology Architecture Technical Framework Technical Architecture Vols 1-2*. The architecture is predicated on selecting standards for a broad and cost-effective infrastructure that provides for reliance on commercial off-the-shelf products as much as possible, is interoperable both within and external to NASA, is flexible for future growth, and is consistent with generally accepted consensus standards as much as feasible. Among these objectives, interoperability is one of NASA’s most critical issues related to IT.

At times, it is in NASA's best interest to specify commercial products as standards for an interoperable implementation of a particular set of related and integrated functions. In those instances, there are often other embedded functions or proprietary extensions within those products whose use may create higher-level interoperability conflicts when embedded in an application system that transcends basic interoperability. For that reason, NASA Centers and programs are advised to apply appropriate caution to the use of proprietary or non-standard extensions, such as features and functions of hardware or software that go beyond the standard functionality.

4.2. Interface and Product Standards. The standards in Table I are established for the components of the office automation software suite and are required based upon both the *Guidance on the Use of Encryption and Digital Signatures for the Protection of Sensitive but Unclassified Information* and NASA-STD-2814.

4.3. Future Interface and Product Standards. The Principal Center for Information Technology Security (PCITS) is working to ensure interoperability with all the latest revisions of the Federal standards and to ensure compliance with Federal standards in all cases (unless a waiver for exemption from such compliance has been approved).

4.4. PGP. The use of PGP within the Agency is required at times to support external partners and some internal operations where the Product Standard cannot support specific platform(s) or application(s) in question. Within NASA, the use of PGP requires using ADK and must operate in the FIPS mode using the listed FIPS-approved algorithms, such as Triple DES.

TABLE I. Interface and Product Standards

Component	Interface Standard	Product Standard
PKI	FIPS PUB 140-2, Security Requirements for Cryptographic Modules, FIPS PUB 46-3 Data Encryption Standard, FIPS PUB 81, DES Modules of Operation, FIPS PUB 171, Key Management Using ANSI X9.17	Entrust CA & RA
Encryption		
Secure Messaging	S/MIME Protocol, FIPS 140-2	Entrust Express - for MS Outlook and Eudora Pro
Secure Web Access		
Strong	SSL 2.0 and SSL 3.0 and GSS-API, utilizing Triple DES, using 168-bit encryption, with SHA-1 message authentication.	Entrust Direct or SSL (using Triple DES with 168 bit encryption)
Medium	SSL 2.0 and SSL 3.0, utilizing RC4 with 128-bit encryption and MD5 message authentication	All Products meeting the Interface standard
Secure Shell replacement for rsh, rlogin, rcp, telnet, rexec, rcp and ftp where reasonable	IETF (Working Draft) Secure Shell (SSH) protocol using Triple DES	Use 1.2.26 or higher with SSH2 recommended
VPN	IPSEC, Triple DES	Cisco-Compatible Systems
Local Disk Encryption	FIPS PUB 46-3, Data Encryption Standard	Entrust Ice
Authentication		
Digital Certificates	X.509 Version 3	Entrust Entelligence
Smart Card Token/Smart Card	FIPS-approved algorithms: DES, Triple DES, DES MAC, DSA/SHA-1, ISO 7816 compliant	N/A
Digital Signature	FIPS PUB 86-2, Digital Signature Standard, FIPS 180-1, Secure Hash Standard	Entrust Entelligence

5. WAIVERS

The conditions under which standards are applicable and the procedures for requesting waivers are contained within each FIPS publication. In 1988, the Secretary of Commerce delegated to the heads of executive departments and agencies the authority to waive mandatory use of FIPS. The process for requesting a waiver to the standards identified in this document is the same as requesting a waiver for a FIPS.

5.1. Request for FIPS Waivers. Under certain exceptional circumstances, the heads of Federal departments and agencies may approve waivers to FIPS. The head of such agency may re-delegate such authority only to a CIO designated pursuant to section 3506 of Title 44, U.S. Code. The NASA CIO is designated as the NASA approving official. Waivers shall be granted only when:

a) Compliance with a standard would adversely affect the accomplishment of the mission of an operator of a NASA computer system, or
b) Cause a major adverse financial impact on the operator that is not offset by Agency-wide savings.

5.2 Process for Handling Waivers. The waiver request should be addressed to the NASA CIO with a copy sent to the PCITS Manager at the Ames Research Center, Moffett Field, CA 94035-1000. Attn: Mail stop 233-17.

NASA may act upon a written waiver request containing the information detailed above. NASA may also act without a written waiver request when the NASA CIO determines that conditions for meeting the standard cannot be met. NASA may approve waivers only by a written decision that explains the basis (findings) on which the Agency head made the decision to grant a waiver. A copy of each such a decision, with procurement sensitive or classified portions clearly identified, shall be sent to:

National Institute of Standards and Technology
ATTN: FIPS Waiver Decisions
Technology Building, Room A216
Gaithersburg, MD 20899.

In addition, notice of each waiver granted and each delegation of authority to approve waivers shall be sent promptly to the Congress and shall be published promptly in the Federal Register.

When the determination on a waiver applies to the procurement of equipment and/or services, a notice of the waiver determination must be published in the Commerce Business Daily as a part of the notice of solicitation for offers of an acquisition or, if the waiver determination is made after that notice is published, by amendment to such notice.

A copy of the waiver, any supporting documents, the document approving the waiver and any supporting and accompanying documents, with such deletions as the agency is authorized and decides to make under 5 U.S.C. Sec. 552(b), shall be part of the procurement documentation and retained by the agency.

5.3 Grandfather Clause. As part of the waiver process, it is recognized that not all existing systems can be transitioned at once. Those systems already in existence can continue to be used until they are replaced as part of their life cycle. Persons or other entities already engaged in an activity prior to the time of this document being approved, not in compliance with these standards, can continue to operate until they can be replaced as part of their life cycle.

6. REVIEW AND REPORTING REQUIREMENTS

6.1. Interoperability Reporting. Each Center CIO will provide the NASA CIO with an annual progress report, as part of the Center's Annual IT Security Plan, outlining the progress made in achieving minimum compliance. Each Center CIO will establish the necessary processes and tools, both manual and automated, to report on an annual basis to the NASA CIO on adherence to this standard for all systems at his or her Center. Centers will maintain sufficient data, internally, as to whether the data and information contained in their systems is secured sufficiently and non-compliance with these standards is documented in the IT System Security Plans. The information to be included in the report to the NASA CIO is as follows:

a. Total number of Special Management Attention (SMA) systems accounts at the Center, broken down between
   1) On-site access only and
   2) Off-site access;

b. Total number of security solutions broken down by the number of:
   1) Secure messaging clients deployed,
   2) Secure web servers used,
   3) SSH clients deployed,
   4) VPN accounts,
   5) Local disk clients deployed,
   6) Applications using digital signatures, and
   7) Smart cards/tokens issued;

c. Total number of waivers requested by number
   1) Approved and
   2) Disapproved

6.2. Interface and Product Standards Review Reporting. PCITS will review this standard on an as-required basis, not to exceed 6-month intervals. The Interface and Product Standards will be updated as required.

7. DURATION

7.1. Duration. This standard will remain in effect until canceled or modified by the NASA CIO.